UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

REDI-DATA, INC., Plaintiff, -against- THE SPAMHAUS PROJECT a/k/a THE SPAMHAUS PROJECT LTD., Defendant.	Case No. 2:20-CV-17484-JMV

DECLARATION OF STEPHEN JOHN LINFORD

I, STEPHEN JOHN LINFORD, British citizen resident of Andorra, declare the following to be true under penalty of perjury:

1. I am the founder and CEO of the Defendant The Spamhaus Project SLU ("The Spamhaus Project"). As such, I am personally familiar with the operations of The Spamhaus Project and with the facts recounted herein.

2. I submit this Declaration in support of The Spamhaus Project's motion to dismiss pursuant to Federal Rule of Civil Procedure 12(b)(2) for lack of personal jurisdiction.

3. The Spamhaus Project was founded in London in 1998. It was originally incorporated and headquartered in the United Kingdom as a British not-for-profit limited liability company -- The Spamhaus Project LTD.

4. In 2019, The Spamhaus Project relocated its headquarters and operations from the United Kingdom to the Principality of Andorra and became a not-for-profit Andorran limited liability company -- The Spamhaus Project S.L.U. The Spamhaus Project is now based in Andorra, with its headquarters and registered Office in Andorra La Vella, Andorra.

5. The Spamhaus Project is a nonprofit organization that tracks spam emails and related cyber threats such as phishing, malware and botnets, and that provides real time, actionable and highly accurate threat intelligence to Internet networks, ISPs and other Internet users worldwide.

6. The Spamhaus Project is run by a dedicated staff of 38 investigators, forensics specialists and network engineers.

7. Among other things, The Spamhaus Project maintains a number of DNS-based Blocklists ("DNSBLs").[1] A DNSBL (commonly known as a "Blocklist") is a database that a provider (such as The Spamhaus Project) creates that lists IP addresses that have been associated with email spam activity. The Spamhaus Project's DNSBLs are maintained on The Spamhaus

---

1 "DNS" refers to the "Domain Name System," which is the Internet's system for converting alphabetic names into numeric IP addresses. For example, when a Web address (URL) is typed into a browser, DNS servers return the IP address of the Web server associated with that name. In this fictional example, the DNS converts the URL www.company.com into the IP address 204.0.8.51. Without DNS, one would have to type the series of four numbers and dots into one's browser to retrieve the website.

Project's servers. Those servers can be searched in real time by Internet mail servers for the purpose of obtaining an opinion on the origin of incoming email received by those Internet mail servers.

8. The role of The Spamhaus Project's DNSBLs is to make available to Spamhaus Users The Spamhaus Project's opinion on whether a particular IP Address meets The Spamhaus Project's own policy for acceptance of inbound email. The Spamhaus Project's DNSBL servers respond to many billions of DNSBL queries from the public every day, and The Spamhaus Project does not charge for access to its DNSBLs.

9. The Spamhaus Project uses the industry standard definition of "spam," which defines spam to mean "unsolicited bulk email" ("UBE"). "Unsolicited" means that the Recipient has not granted verifiable permission for the message to be sent. "Bulk" means that the message is sent as part of a larger collection of messages, all having substantively identical content. An email message is "spam" only if it is both unsolicited and bulk. The Spamhaus Project's identification of spam is focused on consent rather than the content of the message. Whether the Unsolicited Bulk Email ("UBE") message is an advertisement, a scam, pornography, or an offer of a free lunch is irrelevant to the question of whether it constitutes spam. If the message is sent unsolicited and in bulk then the message is spam. Whether the sending of spam is legal or illegal in any particular jurisdiction is

irrelevant. Thus, arguments or assertions as to whether Unsolicited Bulk Email messages are compliant with the requirements set forth in the U.S. "CAN-SPAM Act" (15 U.S.C. § 7701, et. seq.) or other statutes is irrelevant to The Spamhaus Project's identification of spam. The Spamhaus Project does not evaluate the content or legality of the contents of an email message. It merely evaluates whether that message constitutes spam by the industry standard definition.

10. Among the DNSBLs maintained by The Spamhaus Project is The Spamhaus Block List ("SBL") Advisory, which is a database of IP addresses from which Spamhaus does not recommend the acceptance of electronic mail. The SBL is searchable in real time by mail systems throughout the Internet, allowing mail server administrators to identify, tag or block incoming connections from IP addresses which The Spamhaus Project deems to be involved in the sending, hosting or origination of spam.

11. The SBL database is maintained by a dedicated team of investigators and forensics specialists working 24 hours a day to list new confirmed spam issues. IP addresses are listed on the SBL because they appear to The Spamhaus Project to be under the control of, used by, or made available for use by spammers and abusers in unsolicited bulk email or other types of Internet-based abuse that threatens networks or users.

12. SBL listings are based on evidence which has satisfied the SBL team that the IP address or IP address range meets its listing criteria. But the listings are advisory: they represent The Spamhaus Project's opinion about activity involving that IP address or IP range. Types of abuse that can lead to SBL listings include all aspects of unsolicited bulk email (spam) and other types of security threats.

13. Another DNSBL maintained by the Spamhaus Project is The Domain Block List ("DBL"). The DBL is a list of domain names with poor reputations. It includes domains which are used in sending unsolicited bulk email or in sending or hosting malware or viruses, as well as other domains with poor reputation due to many heuristics. The DBL is maintained by a dedicated team of specialists using various data from many sources to craft and maintain a large set of rules controlling an automated system that constantly analyses a large portion of the world's email flow and the domains in it. Most DBL listings occur automatically.

14. The DBL is published in a domain DNSBL format on The Spamhaus Project's servers, and it is searchable in real-time, just like The Spamhaus Project's other DNSBLs. Those running mail server software capable of scanning email headers and message bodies for URIs can use the DBL to identify, classify, or reject mail containing DBL-listed domains.

15. The Spamhaus Project provides procedures for requesting delisting or removal from its DNSBLs. If the issues that caused the listing are resolved and are sufficiently corrected to prevent further abuse, the Spamhaus Project will remove the relevant IP address or domain from the DNSBL.

16. The Spamhaus Project does not itself block any email traffic or prevent anyone from sending emails on the Internet. It is the policies of the particular entity receiving inbound email (the "Receiver") that governs whether particular messages are blocked, delivered, sent to a spam folder, or subjected to additional screening. Every Internet network that chooses to consult a DNSBL (such as those made available by The Spamhaus Project) as part of its spam filtering process is, by doing so, making its own policy decision governing acceptance and handling of inbound email. The Receiver unilaterally makes the choices on whether to search DNSBLs, which DNSBLs to use, and what to do with an incoming email if the email message's originating IP Address is "listed" on the DNSBL.

17. The Spamhaus Project is not engaged in continuous activities purposefully directed to New Jersey.

18. The Spamhaus Project does not do business in New Jersey, and The Spamhaus Project conducts no marketing in New Jersey.

19. The Spamhaus Project is incorporated in the Principality of Andorra and has its principal place of business there. It has no office or employees in New Jersey, and it conducts no business there.

20. The Spamhaus Project has not engaged in any activity in New Jersey, and it is not at home there.

21. The Spamhaus Project had no relationship with Plaintiff Redi-Data, Inc. ("Redi-Data") and did not know where Redi-Data was incorporated or where its physical headquarters or operations were located.

22. The Spamhaus Project did not know that any alleged harm suffered by Redi-Data would be felt in New Jersey.

23. The Spamhaus Project's actions in connection with placing Redi-Data's IPs and domain names on the SBL and the DBL were not actions that The Spamhaus Project aimed or targeted at New Jersey. The SBL and the DBL are not targeted at New Jersey. They are placed on The Spamhaus Project's servers and are available to be searched by anyone in the world with a connection to the Internet.

24. This declaration is signed in a manner that, if falsely made, could subject me to a criminal penalty in the country where the Declaration is signed.

I declare under penalty of perjury under the laws of the United States and of the Principality of Andorra that the forgoing is true and correct.

Dated: Andorra La Vella, Andorra
December 22, 2021

STEPHEN JOHN LINFORD